(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 199 14 506 A 1**

(51) Int. Cl.[7]:
H 04 L 9/32
G 07 F 7/10

(21) Aktenzeichen: 199 14 506.7
(22) Anmeldetag: 30. 3. 1999
(43) Offenlegungstag: 12. 10. 2000

(71) Anmelder:
Siemens AG, 80333 München, DE

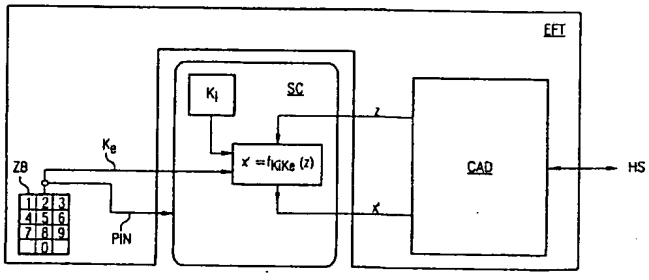
(72) Erfinder:
Blöcher, Uwe, 82178 Puchheim, DE; Munzert, Michael, 80639 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Sicherungsverfahren zur Absicherung der Kommunikation zwischen einer mobilen Datenträgereinrichtung und einem beliebigen System unter Verwendung Datenträgereinrichtungs-externer Informationen

(57) Sicherungsverfahren zur Absicherung der Kommunikation zwischen einer mobilen Datenträgereinrichtung und einem beliebigen System unter Verwendung datenträgereinrichtungsexterner Informationen.
Bei einem Sicherungsverfahren zur Absicherung der Kommunikation zwischen einer mobilen Datenträgereinrichtung, wie z. B. einer Smart Card, und einem beliebigen System, wie z. B. einem Bankterminal, wird zur Erhöhung der Sicherheit gegen Brechen des Sicherungsverfahrens ein Schlüssel gebildet, der nur bei Kombination eines in der Datenträgereinrichtung abgelegten Schlüssels k_i mit einem in die Datenträgereinrichtung eingegebenen Schlüssels k_e gegeben ist.



DE 199 14 506 A 1

DE 199 14 506 A 1

Beschreibung

Der Anmeldungsgegenstand betrifft ein Verfahren zur Authentifikation eines Benutzers und/oder Aufbau einer kryptografischen Kommunikation und/oder verschlüsselten Informationsübertragung mit den Merkmalen des Oberbegriffs des Anspruchs 1.

In heutigen Systemen, wie sie beispielsweise in IEEE Communications Magazine, Vol. 29, No 6 (June 1991), S. 42–48, "Cryptographic Identification Methods for Smart Cards in the process of Standardization" beschrieben sind, wird ein sicherer Kanal zwischen einer Datenträgereinrichtung und einem System mittels Informationen aufgebaut, die auf der Datenträgereinrichtung gespeichert sind. Es gehen benutzerseitig Datenträgereinrichtung-externe Informationen (z. B. PIN) nur ein, um die Funktionalität der Datenträgereinrichtung freizuschalten bzw. zu autorisieren.

Eine wesentliche Bedrohung für Datenträgereinrichtung – basierte Systeme besteht darin, daß mit genügend großem Aufwand die auf der Datenträgereinrichtung gespeicherten Daten ausgelesen werden können und gegebenenfalls modifiziert werden können (z. B. Umgehen einer PIN-Abfrage). Damit können heutige Systeme gebrochen werden.

Dem Anmeldungsgegenstand liegt das Problem zugrunde, die kryptographische Sicherung der Kommunikation (z. B. Datenträgereinrichtung-Authentifikation, Vertraulichkeit, Integrität, Authentifikation des Datenursprungs) zwischen einer Datenträgereinrichtung (z. B. Chipkarte) und einem System (z. B. PC, Server oder Bankterminal) zu erhöhen.

Das Problem wird bei einem durch die Merkmale des Oberbegriffs umrissenen Gegenstand durch die Merkmale des kennzeichnenden Teils des Anspruchs 1 gelöst.

Der Anmeldungsgegenstand stellt sicher, daß das Auslesen der auf der Datenträgereinrichtung gespeicherten Daten nicht zum Erfolg führt. Ein Angreifer benötigt nämlich zusätzliche, Datenträgereinrichtungs-externe Informationen. Damit ist prinzipiell eine deutlich höhere Sicherheit derartiger Systeme möglich.

Vorteilhafte Weiterbildungen des Anmeldungsgegenstandes sind in den Unteransprüchen angegeben.

Gemäß einer besonderen Weiterbildung des Anmeldungsgegenstandes wird die personenspezifische Ziffernfolge PIN (für: Personal Identification Number) als externer Schlüssel k_e verwendet. Diese Maßnahme bringt eine Erhöhung der Sicherheit der Kommunikation ohne Einschränkung des Benutzungskomforts für den Benutzer mit sich.

Der Anmeldungsgegenstand wird im folgenden als Ausführungsbeispiel in einem zum Verständnis erforderlichen Umfang anhand von Figuren näher erläutert. Dabei zeigen:

Fig. 1 eine Anordnung, in der der Anmeldungsgegenstand realisiert ist, und

Fig. 2 Abläufe zwischen den Teilen der Anordnung.

In den Figuren bezeichnen gleiche Bezeichnungen gleiche Elemente.

Fig. 1 zeigt eine mobile Datenträgereinrichtung SC (für: smart card), die in eine Systemeinheit EFT (für: electronic fund terminal) eingeführt ist und mit ihr in Wirkverbindung steht. Die Datenträgereinrichtung mag durch eine Chipkarte im Scheckkartenformat, eine Smart Card oder ein sonstiges benutzerspezifisches Token gegeben sein. Die Systemeinheit mag durch einen elektronischen Bankautomaten zur Geldausgabe, ein electronic fund terminal, ein mobiles funkgestütztes Kommunikationsendgerät, wie z. B. ein Mobiltelefon, ein beliebiges Kommunikationsendgerät oder eine Datenverarbeitungseinrichtung, wie z. B. ein Personal Computer, ein Notebook, ein Laptop oder ein Personal Digital Assistent gegeben sein.

Die Datenträgereinrichtung und die Systemeinheit können auch durch einen Halbleiterchip aufweisenden Schlüssel, der mit einem Schloß eine Wirkverbindung eingeht, oder eine wie eine Armbanduhr getragene Identifikationseinrichtung, die mit einer Zugangssperre eine Wirkverbindung eingeht, gegeben sein.

Im weiteren wird die Erfindung am Beispiel einer mit einem Eingabeterminal in Wirkverbindung stehenden Chipkarte beschrieben.

Wird die Datenträgereinrichtung in die Systemeinheit eingeschoben und damit mit ihr in Wirkverbindung gebracht, wird eine nicht näher dargestellte Identifikationskennung I aus der Datenträgereinrichtung in eine in der Systemeinheit angeordnete Karten-Aufnahme-Einrichtung CAD (für: Card Adaption Device) zur Prüfung der Datenträgereinrichtung auf Echtheit ausgelesen. Im übrigen ist die Karten-Aufnahme-Einrichtung mit einem zentralen System HS (für: host system), mit dem sie Daten auszutauschen vermag, verbunden.

Nach erfolgreicher Echtheitsprüfung der Datenträgereinrichtung gibt der Benutzer sein spezifisches Charakteristikum beispielsweise in die Eingabeeinrichtung der Systemeinheit ein. Das Charakteristikum kann durch eine personenspezifische Ziffernfolge PIN (für: Personal Identification Number) oder einen biometrischen Prozeß, wie z. B. einen Fingerabdruck gegeben sein. Die Eingabeeinrichtung kann durch einen Tastaturblock TB oder einen berührungssensitiven Bildschirm gegeben sein. Der Fingerabdruck kann auch in einen unmittelbar auf der Datenträgereinrichtung angeordneten Fingerabdrucks-Sensor (fingerprint sensor) eingegeben werden. Das eingegebene Charakteristikum wird in der Datenträgereinrichtung mit einem in der Karte abgelegten Identifikationswert CIV (für: Card Identification Value) auf Übereinstimmung verglichen. Bei erfolgreichem Vergleich identifiziert sich der Benutzer gegenüber der Datenträgereinrichtung.

Zur Überprüfung der Authentizität der Datenträgereinrichtung durch die Systemeinheit sendet die Karten-Aufnahme-Einrichtung CAD eine Zufallszahl (random) Z an die Datenträgereinrichtung. Eine Verschlüsselungsfunktion liefert als Ergebnis X' die Verschlüsselung der Zufallszahl Z mit einem in der Datenträgereinrichtung abgelegten internen, Datenträgereinrichtungs-spezifischen Schlüssel k_i. Das Ergebnis X' wird an die Datenträgereinrichtung gesendet, wo eine Überprüfung auf Gleichheit mit dem erwarteten Ergebnis erfolgt. Ergibt die Überprüfung, daß die Gleichheit gegeben ist, wird die Datenträgereinrichtung von der Systemeinheit als authentisiert akzeptiert.

Eine mögliche Manipulation zur Überwindung der vorgesehenen Sicherheitsmaßnahmen fußt auf der Ausspähung des internen Schlüssel k_i.

Anmeldungsgemäß ist vorgesehen, daß der Benutzer zu dem in der Datenträgereinrichtung vorliegenden internen Schlüssel k_i einen zusätzlichen Schlüssel k_e eingibt. Die Eingabe mag an der Systemeinheit, beispielsweise durch Eingabe alphanumerischer Zeichen in einen Tastaturblock TB oder einen berührungssensitiven Bildschirm beziehungsweise durch einen biometrischen Prozeß, wie z. H. einen Fingerabdruck oder Abtastung des Augenhintergrunds (Irisscan), gegeben sein. In einer anderen Ausführungsform wird der zusätzliche Schlüssel k_e in die mobile Datenträgereinrichtung eingegeben, wobei vorzugsweise alphanumerische Zeichen bzw. der Fingerabdruck des Benutzers in einen unmittelbar auf der Datenträgereinrichtung angeordneten Fingerabdrucks-Sensor eingegeben wird.

Der in der Datenträgereinrichtung abgelegte erste Schlüssel k_i bildet einen ersten Teilschlüssel und der zweite Schlüssel k_e bildet einen zweiten Teilschlüssel, wobei die

Kombination des ersten Schlüssels k_i und des zweiten Schlüssels k_e den Schlüssel zur Verschlüsselung der Zufallszahl bilden.

Die Kombination des ersten Schlüssels k_i und des zweiten Schlüssels k_e mag durch Aneinanderfügen ihrer binären Werte erfolgen.

Anmeldungsgemäß ist eine Identifikation und/oder Aufbau einer kryptografischen Kommunikation/verschlüsselten Informationsübertragung nur dann gegeben, wenn die Kombination des ersten Schlüssel k_i und des zweiten Schlüssel k_e vorliegt.

Fig. 2 zeigt Abläufe t zwischen den Teilen des Systems. Ein Benutzer Ur (für: User) gibt seinen Schlüssel k_e ein, der, wie durch einen Pfeil dargestellt, in die mobile Datenträgereinrichtung SC weitergeleitet wird. In der Datenträgereinrichtung wird ein gemeinsamer Schlüssel K_{tok} als Funktion f des in der Datenträgereinrichtung abgelegten Schlüssels k_i und des vom Benutzer eingegebenen Schlüssels k_e gebildet.

Die Funktion f mag durch HMAC und Hashfunktion (z. B. RFC (Request for Comments)2104) beziehungsweise durch einen symmetrischen Kryptoalgorithmus (z. B. DES (Data Encription Standard), IDEA) mit geeignetem Modus (z. B. CBC-Modus) gegeben sein.

Eine Authentifikation/kryptografische Kommunikation/verschlüsselte Informationsübertragung SCOM (für: secure Communikation) zwischen der Datenträgereinrichtung und dem System EFT ist nur dann gegeben, wenn der erste Schlüssel k_i mit dem zweiten Schlüssel k_e zum richtigen, gemeinsamen Schlüssel K_{tok} kombiniert wird.

Patentansprüche

1. Verfahren zur Authentifikation eines Benutzers und/oder Aufbau einer kryptografischen Kommunikation und/oder verschlüsselten Informationsübertragung demzufolge
   - eine mobile Datenträgereinrichtung (SC), insbesondere eine Speicherkarte, mit einem System, insbesondere Eingabeterminal (EFT), in Wirkverbindung gebracht wird,
   - die mobile Datenträgereinrichtung einen ersten Schlüssel k_i innehat,

   dadurch gekennzeichnet, daß
   - der Benutzer einen zweiten Schlüssel k_e eingibt und
   - eine Authentifikation/kryptografische Kommunikation/verschlüsselte Informationsübertragung nur dann gegeben ist, wenn der erste Schlüssel mit dem zweiten Schlüssel kombiniert wird.

2. Verfahren nach Anspruch 1 dadurch gekennzeichnet,
   - der Benutzer ein Charakteristikum an das System zur Authentifikation eingibt,

3. Verfahren nach Anspruch 2 dadurch gekennzeichnet,
   - das Charakteristikum durch eine Persönliche Identifikationsnummer gegeben ist.

4. Verfahren nach einem der vorstehenden Ansprüche dadurch gekennzeichnet,
   - der zweite Schlüssel k_e durch die Persönliche Identifikationsnummer gegeben ist.

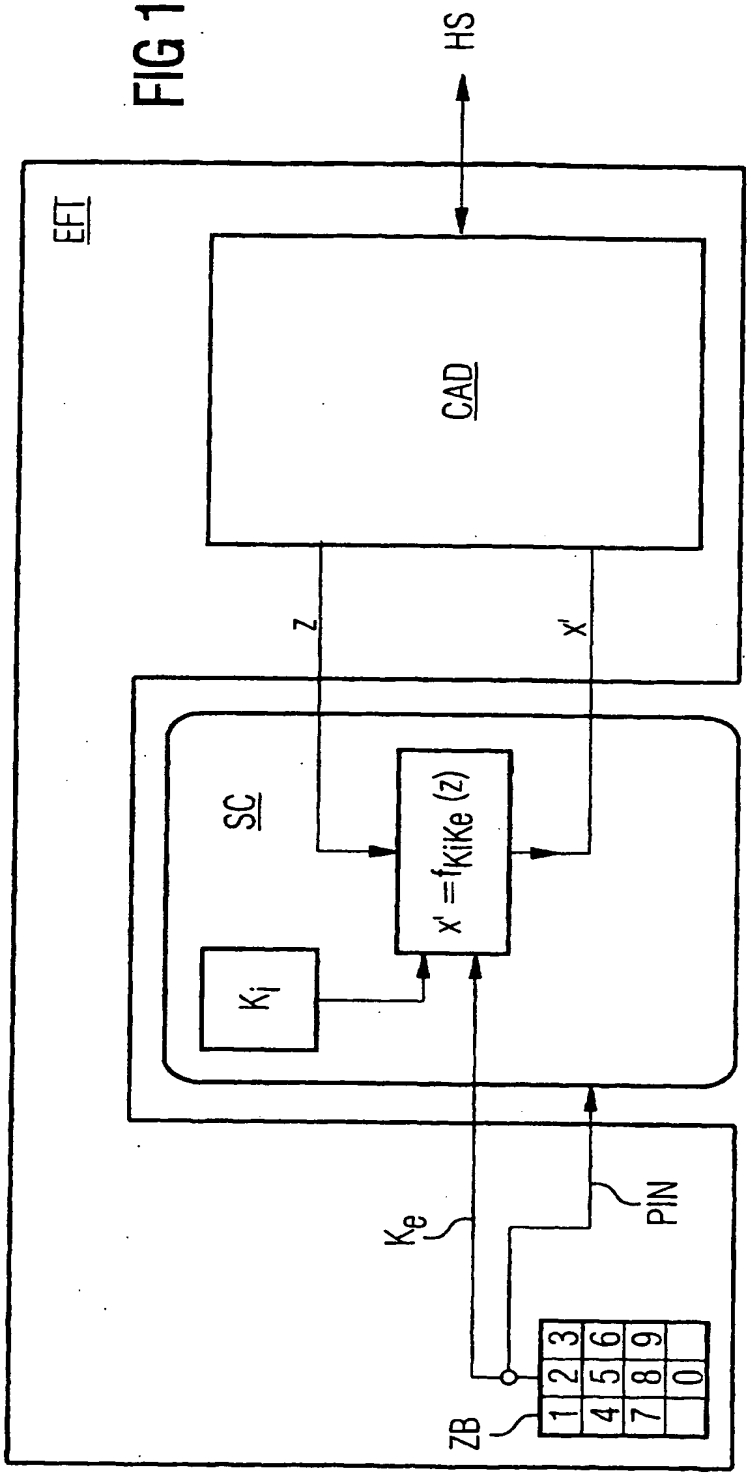
5. Verfahren nach einem der vorstehenden Ansprüche dadurch gekennzeichnet,
   - der zweite Schlüssel k_e durch ein biometrisches Muster gegeben ist.

Hierzu 2 Seite(n) Zeichnungen

- Leerseite -

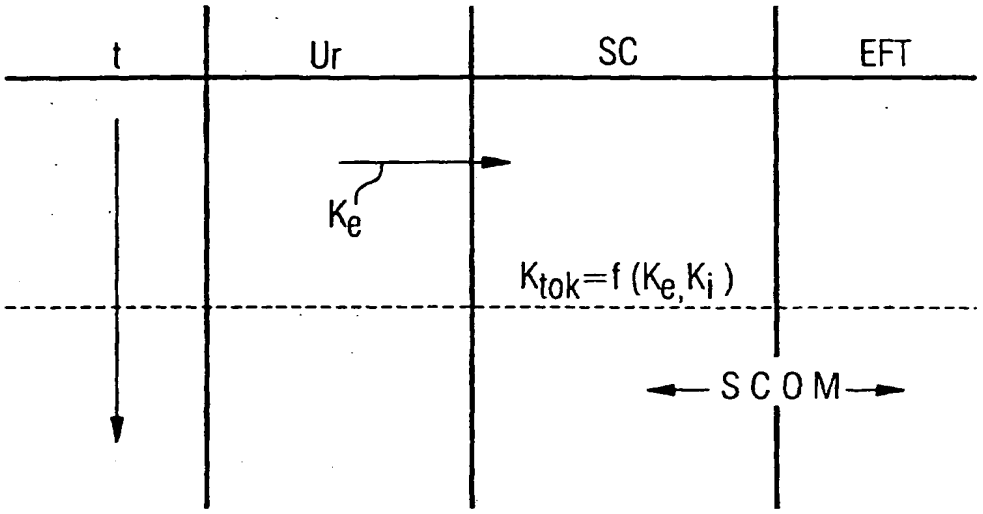
Nummer: DE 199 14 506 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 12. Oktober 2000

FIG 1



Nummer: DE 199 14 506 A1
Int. Cl.[7]: H 04 L 9/32
Offenlegungstag: 12. Oktober 2000

FIG 2



Protection method for communication between mobile data carrier device, such as m mory card, and e.g. input t rminal

Patent Number: DE19914506
Publication date: 2000-10-12

Inventor(s): BLOECHER UWE (DE); MUNZERT MICHAEL (DE)
Applicant(s): SIEMENS AG (DE)

Requested Patent: ☐ DE19914506
Application Number: DE19991014506 19990330
Priority Number(s): DE19991014506 19990330
IPC Classification: H04L9/32; G07F7/10
EC Classification: G07F7/10E, H04L9/32
Equivalents:

Abstract

A user protection procedure provides authentification of the user and/or of the setting-up of a cryptographic communication and/or encrypted information transmission, as a result of which, a mobile (portable) data carrier device (SC), esp. a memory card. The method is set into operative interaction with a system, esp. an input terminal (EFT). The mobile (portable) data carrier device holds a first key (ki). The given user inputs a second key (ke)and an authentification-cryptographic communication-encrypted information transmission is only then given if the first key combines with the second key. The user provides a personal characteristic by way, specifically, of a PIN number.

DOCKET NO: P2001,0201
SERIAL NO: 10/667,567
APPLICANT: Bolker et al.

LEPPER AND GREENBERG P.A.
P.O. BOX 2480
HOLLYWOOD, FLORIDA 33022
TEL. (954) 925-1100